CLAIMS:

1. In a method for providing secure authentication using digital certificates, an improvement to enable the selective transfer of authentication data comprising:
   - presentation of basic authentication data certified by an accepted certifying authority, at the commencement of a secure transaction,
   - transfer of additional individual authentication data units against specific requests, as and when required,

   thereby eliminating the risks associated with providing any authentication data that is not required for a particular transaction.

2. The improved method as claimed in claim 1 wherein the authenticity of said additional individual authentication data is established by using the public key provided in said basic authentication data.

3. The improved method as claimed in claim 1 wherein the authenticity of said additional individual authentication data is established by signature of said accepted certifying authority.

4. The improved method as claimed in claim 1 wherein said additional individual authentication data is provided without the need for establishing a separate session.

5. The improved method as claimed in claim 1 further comprising the facility to invalidate previously presented authentication data and present new authentication data and present new authentication data as and when required, thereby enabling establishment of new transactions without the need for closing an existing session.

6. In a system for providing secure authentication using digital certificates, an improvement to enable the selective transfer of authentication data comprising:
   - means for presenting basic authentication data certified by an accepted certifying authority, at the commencement of a secure transaction,
   - means for transferring additional individual authentication data units against specific requests, as and when required,

thereby eliminating the risks associated with providing any authentication data that is not required for a particular transaction.,

7. The improved system as claimed in claim 6 wherein the authenticity of said additional individual authentication data is established by using the public key provided in said basic authentication data.

8. The improved system as claimed in claim 6 wherein the authenticity of said additional individual authentication data is established by means of signature of said accepted certifying authority.

9. The improved system as claimed in claim 6 wherein said additional individual authentication data is provided without the need for establishing a separate session.

10. The improved system as claimed in claim 6 further comprising the means for invalidating previously presented authentication data and present new authentication data and present new authentication data as and when required, thereby enabling establishment of new transactions without the need for closing an existing session.

11. In a computer program product comprising computer readable program code stored on computer readable storage medium embodied therein for providing secure authentication using digital certificates, an improvement to enable the selective transfer of authentication data comprising:

- computer readable program code means configured for presenting basic authentication data certified by an accepted certifying authority, at the commencement of a secure transaction,
- computer readable program code means configured for transferring additional individual authentication data units against specific requests, as and when required,

thereby eliminating the risks associated with providing any authentication data that is not required for a particular transaction.

12. The improved computer program product as claimed in claim 11 wherein the

authenticity of said additional individual authentication data is established by using the public key provided in said basic authentication data.

13. The improved computer program product as claimed in claim 11 wherein the authenticity of said additional individual authentication data is established by signature of said accepted certifying authority.

14. The improved computer program product as claimed in claim 11 wherein said additional individual authentication data is provided without the need for establishing a separate session.

15. The improved computer program product as claimed in claim 11 further comprising the computer readable program code means configured for invalidating previously presented authentication data and present new authentication data and present new authentication data as and when required, thereby enabling establishment of new transactions without the need for closing an existing session.